UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Technical Conference on Critical Infrastructure Protection Issues Identified in Order No. 791

Prepared Statement of Melanie Seader, Senior Cyber & Infrastructure Security Analyst Edison Electric Institute

April 29, 2014

Good afternoon members of the Commission Staff. I am Melanie Seader, the Senior Cyber & Infrastructure Security Analyst at the Edison Electric Institute (EEI), and am here today representing EEI and our member companies. We appreciate the Commission holding this conference.

EEI is the association of the nation's shareholder-owned electric utilities and its affiliates world-wide. Its members own or operate approximately 70% of the electric industry assets in this country. In addition, its members include Generator Owners and Operators, Transmission Owners and Operators, Load-Serving Entities, and other entities that are subject to mandatory Reliability Standards developed and enforced by the North American Electric Reliability Corporation.

The Critical Infrastructure Protection Reliability Standards (CIP) address cybersecurity to "provide for reliable operation of the bulk-power system."[1] As the Commission stated in Order No. 791, CIP version 5 is "an improvement over the current Commission-approved CIP Reliability Standards" that "adopt[s] new cybersecurity controls and extend[s] the scope of the systems that are protected by the CIP Reliability Standards."[2]

---

1 16 U.S.C. § 824o (a)(3) (2012).

2 Version 5 Critical Infrastructure Protection Reliability Standards, Order No. 791, 78 Fed. Reg. 72,577 (Dec. 3, 2013), 145 FERC ¶ 61,160 (2013) PP 1, 41.

The Low-Medium-High Impact categorization and the "identify, assess, and correct" language used in CIP version 5 is based on the National Institute of Standards and Technology (NIST) Risk Management Framework.[3] The NIST Risk Management Framework "is a methodology for implementing risk management activities into the system development life cycle" of federal information systems that support organizational mission and business processes.[4]

In February 2014, NIST published the *Framework for Improving Critical Infrastructure Cybersecurity* (NIST Cybersecurity Framework). EEI and our member companies were engaged throughout the development of the Framework and supported NIST's development of a flexible, voluntary tool that leverages existing cybersecurity approaches. Also, through the Electric Subsector Coordinating Council (ESCC) we are now coordinating with the Department of Energy to develop sector specific guidance on implementing the Framework, which will include existing energy sector-specific standards used by the electric power industry (e.g., the Electricity Subsector Cybersecurity Capability Maturity Model).

The NIST Cybersecurity Framework "provides organization and structure to today's multiple approaches to cybersecurity." It is a voluntary, risk-based framework to help critical infrastructure organizations build "a consistent and iterative approach to identifying, assessing, and managing cybersecurity risk."[5]

In the Cybersecurity Framework, NIST recognized that implementation is not a "one-size-fits-all approach" as risk is unique to the different sectors and organizations within each sector. As a result, "the tools and methods used to achieve the outcomes described by the

---

3 *Id*. at PP 14-15.

4 Kelley Dempsey, National Institute of Standards and Technology, *Summary of NIST 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations*, February 2014, available at: http://csrc.nist.gov/publications/nistpubs/800-53-rev4/sp800-53r4_summary.pdf (accessed 4/28/14).

5 National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* Version 1.0.

Framework will vary." The use of the Framework's cybersecurity activities are guided by an organization's risk management processes, legal and regulatory processes, business and mission objectives, and organizational constraints. This flexible approach enables organizations to "determine activities that are important to critical service delivery" and "prioritize investments to maximize the impact of each dollar spent."[6]

These three approaches—CIP version 5, the NIST Risk Management Framework, and the NIST Cybersecurity Framework—all address cybersecurity; however, each is very different. For example:

1. CIP version 5 is focused on the impact to bulk-power system reliability. The NIST Risk Management Framework is focused on the impact to confidentiality, integrity, and availability of federal government information and information systems. The NIST Cybersecurity Framework is focused on reducing cybersecurity risk to critical infrastructure—sixteen sectors with very diverse cybersecurity risk profiles.

2. CIP version 5 is mandatory and enforceable for bulk-power system owners and operators. The NIST Risk Management Framework is mandatory for Federal agencies. The NIST Cybersecurity Framework is voluntary for critical infrastructure asset owners and operators.

3. CIP version 5 is compliance-based, requiring bulk-power system asset owners and operators to document, report, and provide compliance evidence to external parties (NERC Regional Entities and FERC) on specific security controls. The NIST Risk Management Framework is risk-based, giving federal agencies discretion in implementing security controls and accepting risk. The NIST Cybersecurity Framework

[6] *Id.*

is also risk-based, giving industry discretion (use of reasonable business judgment) in implementing security controls and accepting risk.

4. Violations of CIP version 5 result in financial penalties to bulk-power system owners and operators. There are no financial penalties associated with the NIST Frameworks, which allow internal auditing—government audits government for the NIST Risk Management Framework and industry audits industry for the NIST Cybersecurity Framework.

5. Because violations to CIP version 5 result in financial penalties, its language must be clear "as to the implementation and compliance obligation it places on responsible entities" and must not "be too vague to audit and enforce."[7] The language of the NIST Frameworks is flexible, allowing its use or implementation to vary among federal agencies and critical infrastructure owners and operators.

CIP version 5 will not guarantee security, but it will protect reliability of the bulk-power system. Voluntary standards and frameworks such as the NIST Frameworks allow electric power companies to enhance their enterprise-wide cybersecurity posture, which exceeds the scope of the systems that are protected by CIP version 5.

The flexibility built into the NIST Frameworks makes it difficult to incorporate risk-based concepts into the clear compliance language needed for the CIP standards. However, much of the work already done to implement earlier versions of the CIP standards will help electric power companies address core portions of the NIST Cybersecurity Framework.

The NIST Cybersecurity Framework can help electric power companies organize the various cybersecurity approaches used within a business unit or throughout an enterprise to identify opportunities for improvement, which can be addressed using risk-based processes. The

[7] *Id.* at PP 4, 35, 45-52, 67-72.

extensibility of this approach enables companies to evolve their security practices in response to the growing threat, while remaining compliant with local, state, and federal security mandates. Another promising benefit of the NIST Cybersecurity Framework is its use as an internal and external communication tool to facilitate cybersecurity discussions among suppliers, management, government, and interdependent sectors.

However, when talking about the NIST Cybersecurity Framework and CIP version 5, it is important to remember that both of these approaches to cybersecurity are new. As the industry gains experience and reaches a steady state in implementing these new voluntary and mandatory approaches to cybersecurity, we will be able to identify strengths and weaknesses based on implementation rather than theory. This experience is essential to strengthening the voluntary and mandatory approaches we use to improve the industry's security and resilience.